Chapter 6: Importance of Strong Enterprise Governance Practices 115

History and Background of Enterprise Governance: A U.S. Perspective 116
Enterprise Integrity and Ethical Behavior 119
Disclosure and Transparency 125
Rights and Equitable Treatment of Shareholders and Key Stakeholders 126
Governance Role and Responsibilities of the Board 128
Governance as a Key Element of GRC 128

Chapter 7: Enterprise Compliance Issues Today 131

Compliance Issues Today 132
Establish a Compliance Assessment Team 133
Compliance Risk Assessments and Compliance Program Reviews 136
Work Unit-Level Compliance Tracking and Review Processes 138
Compliance-Related Procedures and Staff Education Programs 141
Enterprise Hotline Compliance and Whistleblower Support 142
Assessing the Overall Enterprise Compliance Program 144

Chapter 8: Integrating ERM with COSO Internal Controls 147

COSO Internal Controls Background and Earlier Legislation 147
Efforts Leading to the Treadway Commission 151
COSO Internal Controls Framework 156
COSO Internal Controls and COSO ERM: Compared 174

Chapter 9: Sarbanes-Oxley and Enterprise Risk Management Concerns 177

Sarbanes-Oxley Act Background 177
SOx Legislation Overview 179
Enterprise Risk Management and SOx Section 404 Reviews 193
Internal Controls Reporting and Materiality 198
PCAOB Risk-Based Auditing Standards 199
Sarbanes-Oxley: The Other Sections 200
SOx and COSO ERM 201

Chapter 10: Corporate Culture and Risk Portfolio Management 203

Whistleblower and Hotline Functions 204
Risk Portfolio Management 208
Integrated Enterprise-Wide Risk Management 211

Chapter 11: OCEG Capability Model GRC Standards 215

GRC Capability Model “Red Book” 215
Other OCEG Materials: The “Burgundy Book” 223
Level and Scope of the OCEG Standards-Setting Authority 224
Chapter 12: Importance of GRC Principles in the Board Room  
- Board Decisions and Risk Management  
- Board Organization and Governance Rules  
- Corporate Charters and the Board Committee Structure  
- Audit Committees and Managing Risks  
- Establishing a Board-Level Risk Committee  
- Audit and Risk Committee Coordination  
- COSO ERM and Corporate Governance  

Chapter 13: Role of Internal Audit in Enterprise Risk Management  
- Internal Audit Standards for Evaluating Risk  
- COSO ERM for More Effective Internal Audit Planning  
- Risk-Based Internal Audit Findings and Recommendations  
- COSO ERM and Internal Audit  

Chapter 14: Understanding Project Management Risks  
- Project Management Process  
- *PMBOK® Guide’s Project Manager Risk Management Approach*  
- Project-Related Risks: What Can Go Wrong  
- Implementing ERM for Project Managers  

Chapter 15: Information Technology and Enterprise Risk Management  
- IT and the COSO ERM Framework  
- IT Application Systems Risks  
- Effective IT Continuity Planning  
- Worms, Viruses, and System Network Risks  
- IT and Effective ERM Processes  

Chapter 16: Establishing an Effective GRC Culture throughout the Enterprise  
- First Steps to Establishing a GRC Culture: An Example  
- Promoting the Concept of Enterprise Risk  
- Establishing of Enterprise-Wide Governance Awareness  
- Enterprise Codes of Conduct  
- Building a GRC Culture: Risk, Governance, and Compliance Education Programs  
- Keeping the GRC Culture Current  

Chapter 17: ISO 31000 and 38500 Risk Management Worldwide Standards  
- ISO Standards-Setting Process  
- Understanding ISO 31000